



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/005,271	12/05/2001	Geoffrey S. Strongin	2000.055700	6634
23720	7590	10/20/2003	EXAMINER	
WILLIAMS, MORGAN & AMERSON, P.C. 10333 RICHMOND, SUITE 1100 HOUSTON, TX 77042			DINH, NGOC V	
			ART UNIT	PAPER NUMBER
			2187	
DATE MAILED: 10/20/2003				

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/005,271	STRONGIN ET AL.	
	Examiner NGOC V DINH	Art Unit 2187	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 05 December 2001.
- 2a) This action is FINAL.                  2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-49 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-49 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) The proposed drawing correction filed on \_\_\_\_\_ is: a) approved b) disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.
- 12) The oath or declaration is objected to by the Examiner.

#### Priority under 35 U.S.C. §§ 119 and 120

- 13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some \* c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) The translation of the foreign language provisional application has been received.
- 15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

#### Attachment(s)

- |  |  |
|--|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                    | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ . |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)           | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ . | 6) <input type="checkbox"/> Other: _____ .                                   |

## **DETAILED ACTION**

### ***Specification***

1. The disclosure is objected to because of the following informalities: Applicant is required to provide the application number for all of the copending applications cited in page 2 of the specification in response to this office action.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 3-4, 7, 10-17, 19-20, 22-23, 26, 29-32, 41-43, 46, 49 are rejected under 35 U.S.C. 102(b) as being anticipated by Hohensee et al PN 5,756,206.

#### **2. As per claims 1, 3-4:**

Hohensee teaches a memory management unit [14, fig. 1] for managing a memory storing data arranged within a plurality of memory pages [fig. 3; col. 2, lines 45-65], the memory management unit comprising:

a security check unit coupled to receive a physical address within a selected memory page and security attributes of the selected memory page, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure [e.g., segment length field (33n), segment base address field (34n), fig. 2] located in the memory to obtain an additional security attribute [e.g., access right field (32n), fig. 2; READ/WRITE access] of the selected memory page, and to generate a fault signal [e.g., ACCESS FAULT; SEG LEN VIOL, fig. 2, col. 8, lines 1-20; PAGE LEN VIOL, fig. 3, col. 11, 40-50; FAULT STATUS REG (83), fig. 4] dependent upon the security attributes of selected memory page and the additional security attribute of the selected memory page [col. 2, lines 40-65; col. 5, lines 32-65; fig. 5, 5A-5B].

Hohensee further teaches the memory management unit, wherein the at least one security attribute data structure comprises a security attribute table directory [TABLE 31, fig. 2], and at least one security attribute table [32(n)-34(n)]; wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry [fig. 2-4; col. 7, line1 to col. 8, line 65; col. 9, line 38 to col. 10 line 65].

**3. As per claim 7, 10:**

Hohensee teaches the memory management unit, wherein the linear address is produced during execution of an instruction residing within a first memory page, and wherein the security check unit is coupled to receive a current privilege level (CPL) [col. 21, lines 38-45; col. 23, line 63 to col. 24 line 7] of a task including the instruction, and wherein the security check logic is configured obtain an additional security attribute of the first memory page from the at least one security attribute data structure, and wherein the security check logic is configured to generate the fault signal dependent upon the CPL of the task including the instruction, the additional security attribute of the first memory page, the security attributes of the selected memory page, and the additional security attribute of the selected memory page; wherein the linear address is produced during execution of an instruction residing within a first memory page, and wherein the security check unit is coupled to receive a value of a secure execution mode (SEM) bit indicative of operation in a secure execution mode, and wherein the security check logic is configured obtain an additional security attribute of the first memory page from the at least one security attribute data structure, and wherein the security check logic is configured to generate the fault signal dependent upon the value of the SEM bit, the additional security attribute of the first memory page, the security attributes of the selected memory page, and the additional security attribute of the selected memory page; wherein the fault signal is a page fault signal as defined by the x86 processor [col. 6, lines

30-35] architecture [col. 5, lines 9-55; col. 7, line 1 to col. 8, line 65; col. 9, line 1 to col. 10, line 60 col. 14, lines 5-65].

**4. As per claims 11-12:**

Hohensee teaches a computer system, comprising:  
central processing unit, comprising:  
an execution unit [11, fig. 1] operably coupled to a memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and a memory management unit (MMU) [14, fig. 1] operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores data arranged within a plurality of memory pages, and wherein the MMU comprises:  
a security check unit coupled to receive a physical address within a selected memory page and security attributes of the selected memory page, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, and to generate a fault signal dependent upon the security attributes of selected memory page and the additional security attribute of the selected memory page [fig. 1-3; col. 2, lines 40-65; col. 5, lines 10-60; fig. 5, 5A-5B; fig. 2-4; col. 7, line 1 to col. 8, line 65; col. 9, line 38 to col. 10 line 65].

**5. As per claims 13 and 30:**

Hohensee teaches a memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising: a paging unit coupled to the memory and to receive a linear address and configured to use the linear address to produce a physical address within a selected memory page, wherein the physical address includes a base address [34(n), fig. 2] of a selected memory page and an offset [37, fig. 2; col. 7, lines 35-40], wherein the paging unit is configured to use the linear address to access at least one paged memory data structure located in the memory to obtain security attributes of the selected memory page, and wherein the paging unit is configured to produce a fault signal dependent upon the security attributes of the selected memory page; and wherein the paging unit comprises a security check unit coupled to receive the physical

address and the security attributes of the selected memory page, and wherein the security check unit is configured to use the physical address of the selected memory page to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, and to generate the fault signal dependent upon the security attributes of selected memory page and the additional security attribute of the selected memory page [fig. 1-3; col. 2, lines 40-65; col. 5, lines 10-60; fig. 5, 5A-5B; fig. 2-4; col. 7, line1 to col. 8, line 65; col. 9, line 38 to col. 10 line 65].

**6. As per claims 14-17, 19-20, 22-23, 26, 29, 31-32, 38-39:**

Hohensee teaches the memory management unit, wherein the paging unit produces physical address of the selected memory page during execution of an instruction residing within a first memory page; the physical address within the selected memory page includes a base address and an offset [col. 2, lines 40-65; col. 2, lines 1-20; col.7, lines 35-50]; paging unit is configured to obtain the base address from the at least one paged memory data structure; at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture [col. 7, lines 13-50; col. 12, lines 31-50]; the paging unit is configured to receive security attribute of the instruction and to produce the fault signal dependent upon the security attribute of the instruction and the security attributes of the selected memory page [col. 5, lines 35-55]; the security attribute of the instruction comprises a current privilege level (CPL) of a task including the instruction as defined by the x86 processor architecture [col. 21, 39-45; col. 23, line 63 to col. 24, line 7]; at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table; the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry [col. 7, lines 13-65; col. 7, line 65 to col. 8, line 45]; the security check unit is coupled to receive the CPL of the task including the instruction, and wherein the security check logic is configured obtain an additional security attribute of the

first memory page including the instruction from the at least one security attribute data structure, and wherein the security check logic is configured to generate the fault signal dependent upon the CPL of the task including the instruction, the additional security attribute of the first memory page including the instruction, the security attributes of the selected memory page, and the additional security attribute of the selected memory page [col. 7, lines 13-65; col. 7, line 65 to col. 8, line 45; col. 21, 39-45; col. 23, line 63 to col. 24, line 7], and the fault signal is a page fault signal as defined by the x86 processor architecture [col. 11, lines 38-50; PAGE LEN VIOL, fig. 3; col. 12, lines 35-40].

**7. As per claims 41-43, 46, 49:**

The claimed elements in the memory management unit in claims 1, 3-4, 7, 10, 13, 14-17, 19-20, 22-23, 26 and 29 are no more than means for carrying out the corresponding steps in the method of claims 41-43, 46 and 46. Therefore, claims 41-43, 46 and 46 are rejected for the same reason as set forth in claims 1, 3-4, 7, 10, 13, 14-1719-20, 22-23, 26 and 29.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2, 18, 34-35, 45 are rejected under 35 U.S.C 103(a) as being unpatentable over Hohensee, and in view of The Admitted Prior Art (APA).

**8. As per claim 2, 18, 34-35:**

Hohensee teaches the claimed limitations as mentioned above.

Hohensee does not teach the security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed

to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

The APA teaches the security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page [fig 2-3].

It would have been obvious to one having ordinary skill in the art at the time the invention was made to further include APA ‘s teaching into Hohensee’s memory management unit. This is because it has been well known in the pertinent art that in Unix system or in window system a user level called “root” or “super-user” or system administrator. A flag (Unix system) or check box (window system) associated with the mentioned user level above is set, then this user level (super-user/supervisor) is responsible for supervising the entire system to ensure the system is safety guarded against unauthorized access to the system. The supervisor further determines whether or not the users have permission to access (that is read only, or read and write) the page by enable/disable the read/write bit in the system to ensure the integrity of the system.

**9. As per claim 45:**

As claim 45, Hohensee teaches the claimed apparatus. Therefore, Hohensee teaches the claimed system for carrying out the method of step.

Claims 5-6, 8, 24-25, 27, 36-37, 40, 47-48 are rejected under 35 U.S.C 103(a) as being unpatentable over Hohensee, and in view of Blonder PN 5,802,275.

**10. As per claims 5-6, 8, 24-25, 27, 36-37, 40:**

Hohensee teaches the claimed limitations as noted above.

Art Unit: 2187

Hohensee does not teach the memory management unit, wherein each entry of the security attribute table includes a secure page (SP) bit, and wherein the SP bit indicates whether or not a corresponding memory page is a secure page.

Blonder teaches a secure page (SP) bit [151, fig. 1], and wherein the SP bit indicates whether or not a corresponding memory page is a secure page [col. 4, lines 15-60].

It would have been obvious to one having ordinary skill in the art at the time the invention was made to further include Blonder 's teaching into Hohensee's memory management unit. Doing so would prevent non-secure programs from corrupting secure programs and their data [abstract; col. 2, lines 10-35].

**11. As per claim 47-48:**

As claims 47-48, Hohensee teaches the claimed apparatus. Therefore, Hohensee teaches the claimed system for carrying out the method of steps.

Claims 9, 21, 28, 33, 44 are rejected under 35 U.S.C 103(a) as being unpatentable over Hohensee, and in view of Slassi PN 6,435,416.

**12. As per claims 9, 21, 28, 33:**

Hohensee teaches the claimed limitations as noted above.

Hohensee does not teach the memory management unit, wherein a value of a secure execution mode (SEM) bit indicative of operation in a secure execution mode

Slassi teaches a value of a secure execution mode (SEM) bit indicative of operation in a secure execution mode [col. 1, lines 50-65; col. col. 3, lines 30-40].

It would have been obvious to one having ordinary skill in the art at the time the invention was made to further include secure execution mode into Hohensee's memory management unit. Doing so would prevent the execution of instructions that enable the computer to access the inputted personal code [Slassi, col. 4, lines 61-63].

**13. As per claim 44:**

As claim 44, Hohensee teaches the claimed apparatus. Therefore, Hohensee teaches the claimed system for carrying out the method of step.

***Conclusion***

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
  - a. Yoshioka et al PN 6,0476354 discloses data processor for implementing virtual pages.
  - b. Mahon et al PN 4,8094160 discloses privilege level checking instruction for secure computer system.
  - c. Worth PN 5,881,225 discloses security monitor for controlling functional access to system.
  - d. Abraham et al PN 5,048,085 discloses transaction system security method.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ngoc Dinh whose telephone number is (703) 305-3023. The examiner can normally be reached on Monday-Friday 8:30 AM-5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Donald A. Sparks, can be reached on (703) 308-1756. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

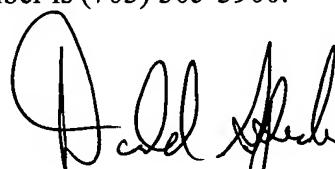


NGOC DINH

Patent Examiner

ART UNIT 2187

October 8, 2003



DONALD SPARKS

Supervisory Patent Examiner

Technology Center 2100